REMARKS

Claims 1-5, 7-9, 11-13, 15 and 16 are pending in this application; and in the Office Action, the Examiner issued a final rejection of these claims under 35 U.S.C. 103 as being unpatentable over the prior art. More specifically, Claims 1, 2, 15 and 16 were rejected as being unpatentable over U.S. Patent 5,878,138 (Yacobi) in view of U.S. Patent 6,298,153 (Oishi). Claims 3-5, 7-9 and 11-13 were rejected as being unpatentable over U.S. Patent 6,675,153 (Cook, et al.) as modified by Oishi.

Applicants herein ask that independent Claims 1, 3, 7 and 11 be amended to better define the subject matters of these claims.

For the reasons discussed below, Claims 1-5, 7-9, 11-13, 15 and 16 patentably distinguish over the prior art and are allowable. The Examiner is thus respectfully requested to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 103, and to allow these claims.

As explained in detail in the present application, this invention provides methods and systems to create and manage digital cash. In accordance with the present invention, a customer sends a request for digital cash to a bank along with a public key of an encryption scheme. The bank signs the cash using a secret key of a digital signature scheme, and then encrypts the signature by using the public key provided by the customer.

The bank also encrypts an unsigned copy of the cash, and the bank sends back to the customer a copy of the encrypted signed cash and a copy of the unsigned cash. The customer then decrypts the signed and unsigned copies of the cash using the private key of the encryption scheme, and can then use the cash for payment to a third party. This third party is then able to check the validity of the digital cash with the bank and can redeem the digital cash for payment.

The present invention has a umber of important features. One such feature is the use of a non-homomorphic signature scheme by the bank. This type of signature scheme allows the customer to receive and use the cash, and allows the third party to redeem the cash, while keeping the identity of the customer secret from the bank. Moreover, all of this can be achieved without having to use a blind signature.

Another important feature of the invention is that the back provides the customer with two encrypted copies of the cash – one that is signed and one that is not signed. With these two copies, a third party can readily determine the amount of the cash without the need to decode the signed copy. That copy can be sent undecoded to the bank, to allow the bank to confirm the legitimacy of the signed copy.

The prior art of record does not disclose or suggest the principal of the bank sending back to the customer both an encrypted signed copy of the cask and an encrypted unsigned copy of the cash.

In particular, Yacobi and Cook, et al. both describe procedures for using electronic cash or electronic assets.

In one specific procedure discussed in Yacobi, a tamper resistant electronic wallet is used to store the asset. This wallet is intended to detect fraud and to eliminate further fraud before the criminal has had an opportunity to profit from the fraud.

Yacobi also discloses, from column 12, line 50 to column 15, line 10, a blind re-certification process; however, this process uses a blind signature, as specifically discussed in column 12, lines 50-64.

Cook, et al. describes a system for authorizing electronic transactions between a consumer and a merchant. One objective of this system is to keep the consumer anonymous to the merchant, not to keep the consumer anonymous from the issuer or certifying authority.

As a review of these references shows, Yacobi and Cook, et al. do not disclose or teach the above-discussed use of two encrypted copies of the cash – one signed and one unsigned.

Oishi discloses various digital signature procedures, including the use of an anonymous public key certificate. As discussed in the present application, non-homomorphic signature schemes are, per se, known. Oishi does not relate to digital cash, and does not provide any suggestion or guidance as to how to use effectively the disclosed cryptographic method in a digital cash system. In particular, Oishi clearly does not address the same specific problem that is effectively addressed by the present invention – to provide secure digital cash that can be used by a customer in a conventional manner while still maintaining the customer's identity anonymous to the bank.

The combined use, in accordance with the teaching of this invention, of the encrypted signed and unsigned copies of the cash enable the present invention to solve effectively this problem.

Claims 1, 3, 7 and 11 describe the above-discussed feature of the invention. For instance, Claim 1 describes the step of sending back to the user both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin. Further, Claims 2, 7 and 11 describe the feature that both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit are sent back to the customer.

As discussed above, this feature of the invention is of utility because when these two copies are given to a third party, that party knows the amount of the unit and also can send the signed copy to the bank to confirm the legitimacy of the unit. And this can be done while maintaining the bank's customer anonymous to the bank.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, are not believed to be any more relevant than Yacobi, Oishi and Cook, et al. In particular, these other references also do not suggest or disclose the use of two copies of the encrypted cask in the above-described manner.

In light of the differences between Claims 1, 3, 7 and 11 and the prior art, and because of the advantages associated with those differences, it cannot be said that any of Claims 1, 3, 7 and 11 would have been obvious to one of ordinary skill in the art. Accordingly, these claims patentably distinguish over the prior art and are allowable. Claim 2 is dependent from, and is allowable with, Claim 1; and Claims 4, 5, 15 and 16 are dependent from Claim 3 and are allowable therewith. Likewise, Claims 8 and 9 are dependent from Claim 7 and are allowable therewith; and Claims 12 and 13 are dependent from, and are allowable with, Claim 11.

It is noted that the changes requested herein to Claims 1, 3, 7 and 11 only elaborate of features already described in the claims. For example, the amendments to Claims 1 and 3 describe in more detail what the user or customer receives and uses in the methods of these claims. Moreover, the last Office Action was the first time that the Examiner applied Oishi against the claims, and it is submitted that Applicants should have an opportunity to respond to this new rejection. It is thus believed that entry of this Amendment is appropriate, and such entry is respectfully requested.

In view of the above-discussion, the Examiner is asked to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-5, 7-9 and 11-13, 15 and 16 under 35 U.S.C. §103, and to allow these claims.

Every effort has been made to place this application in condition for allowance, a notice of which is requested. If the Examiner believes that a telephone conference with

Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343
JSS:gc